(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平6－188877

(43)公開日　平成６年(1994)７月８日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/06					
	9/14					
Ｇ０９Ｃ	1/00		8837－5L			
Ｈ０４Ｂ	7/26	１０９　Ｒ	7304－5K			
			7117－5K	Ｈ０４Ｌ	9/ 02	Ｚ

審査請求　有　　請求項の数24(全 14 頁)

(21)出願番号　特願平4－267808

(22)出願日　平成４年(1992)９月11日

(31)優先権主張番号　785,039

(32)優先日　1991年９月13日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　390035493
アメリカン　テレフォン　アンド　テレグラフ　カムパニー
AMERICAN TELEPHONE AND TELEGPAPH COMPANY
アメリカ合衆国　10013－2412　ニューヨーク　ニューヨーク　アヴェニュー　オブ　ジ　アメリカズ　32

(74)代理人　弁理士　三俣　弘文

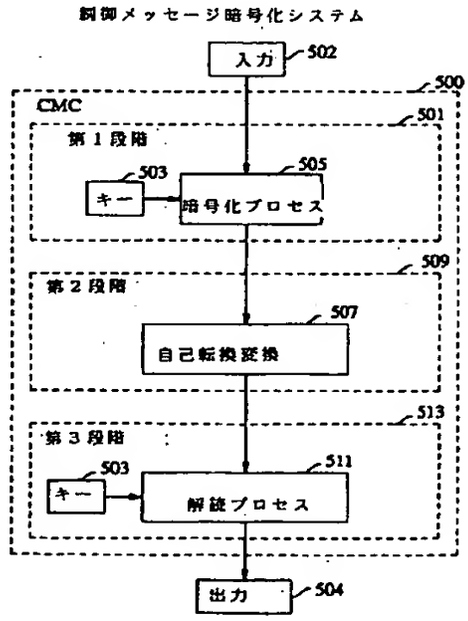
最終頁に続く

(54)【発明の名称】　暗号化システム

(57)【要約】

【目的】　セルラー電話システムにおける暗号システムにおいて、可変長の元メッセージを、８ビットマイクロコンピュータによって簡単に暗号化及び解読を行うことが可能な、比較的安全な、自己転換、対称キー暗号システムを提供することを目的とする。

【構成】　８ビットマイクロコンピュータで効率よく実効可能な、比較的安全で、自己転換、対称キー暗号システムによるキー暗号システムに関する。本暗号システムは、セルラー電話への応用に特に適している。本暗号システムは、３つの段階から構成される：１）自動キー暗号化、２）第１段階で暗号化されたメッセージの一部から導出されたキーを用いた、１回限り暗号通信法の利用、３）第１とは逆の第２の自動キー解読からなる。



1

【特許請求の範囲】

【請求項1】　通信システムにおいて、メッセージを表すメッセージ信号の集合を変換する方法において、

第1の中間信号の集合を形成するために、暗号化プロセス（505）およびキー信号の集合（503）によって前記メッセージ信号の集合を暗号化するステップと、

第2の中間信号の集合を形成するために、インボリュート変換（507）に従って前記第1中間信号の集合を変更するステップと、

出力信号の集合を形成するために、前記暗号化プロセスの逆である解読プロセス（511）によって、前記第2中間信号の集合を解読するステップとを有し、

前記変更ステップが、前記第1中間信号の集合の第1の部分集合に基づいた非キー変換によって、前記第1の中間信号の集合の第2の部分集合を修正するステップからなることを特徴とする暗号化方法。

【請求項2】　前記暗号化ステップが、第1の自動キープロセスに従った、前記第1の中間信号を形成するステップを有し、前記解読ステップが、第2の自動キープロセスに従った、前記出力信号を形成するステップを有することを特徴とする、請求項1に記載の暗号化方法。

【請求項3】　ソース信号の集合から、前記キー信号の集合を導出するステップを有することを特徴とする、請求項1に記載の暗号化方法。

【請求項4】　前記導出ステップが、前記キー信号の集合を形成するために、前記ソース信号の集合とともに、パターン信号の集合をハッシュするステップからなることを特徴とする、請求項3に記載の暗号化方法。

【請求項5】　前記キー信号の集合および前記パターン信号の集合が、Nを正の整数として、N個の要素をそれぞれ有することを特徴とする、請求項4に記載の暗号化方法。

【請求項6】　前記導出ステップが、前記ハッシュステップで用いることのできる、前記パターン信号の集合を作成するステップを有することを特徴とする、請求項5に記載の暗号化方法。

【請求項7】　NおよびDを正の整数として、前記キー信号の集合がN個の要素を有し、メッセージ信号の集合がD個の要素を有することを特徴とする、請求項1に記載の暗号化方法。

【請求項8】　前記メッセージ信号の集合を暗号化する前記ステップが、

信号zを選択された大きさに設定するステップと、

0≦i＜Dの範囲の相異なる整数値信号iに対し、

前記信号iおよびzの各大きさに基づいて信号qを設定するステップと、

信号kを、前記信号qおよびT［q］（ただしT［q］は前記キー信号の集合のq番目の要素）の各大きさに基づいて設定するステップと、

前記第1の中間信号の集合のi番目の要素を、前記メッセージ信号の集合の前記第i要素および前記信号kの各大きさに基づいて生成するステップと、

前記信号zの大きさを、前記第1の中間信号の集合の第i要素および前記信号zの各大きさに基づいて更新するステップとからなることを特徴とする、請求項7に記載の暗号化方法。

【請求項9】　前記メッセージ信号の集合を暗号化する前記ステップが、

nビット信号zを選択された大きさに設定するステップと、

0≦i＜Dの範囲の連続する整数値をとるインデックスiに対し、

nビット信号qをz＃mに（ただし、＃はビットごとのブール排他的OR演算子であり、mはi　mod　2^n）設定するステップと、

nビット信号kをT［q］に（ただしT［q］は前記キー信号の集合のnビット要素）設定するステップと、

前記メッセージ信号の集合の前記i番目のnビット要素とnビット信号kを、2^nを法として加算することによって、前記第1の中間信号の集合のi番目のnビット要素を生成するステップと、

前記第1の中間信号の集合の前記i番目のnビット要素とnビット信号zを、2^nを法として加算することによって、前記nビット信号zの大きさを更新するステップとからなることを特徴とする、請求項7に記載の暗号化方法。

【請求項10】　前記各nビットが8ビットであり、2^nが256に等しいことを特徴とする、請求項9に記載の暗号化方法。

【請求項11】　前記第1の中間信号の前記変更ステップが、0≦i＜（D－1）／2の範囲で、b（i）＃qに等しい前記第2の中間信号の集合のi番目の要素を生成する（ただし、b（i）は前記第1の中間信号の集合のi番目の要素、qはb（x）に基づき、xはDおよびiの値に基づき、b（x）は前記第1の中間信号の集合のx番目の要素で、＃はビットごとのブール排他的OR演算子）ステップからなることを特徴とする、請求項7に記載の暗号化方法。

【請求項12】　前記第2の中間信号の集合を解読する前記ステップが、

信号zを選択された大きさに設定するステップと、

0≦i＜Dの範囲の相異なる整数値信号iに対し、

前記信号iおよびzの各大きさに基づいて信号qを設定するステップと、

信号kを、前記信号qおよびT［q］（ただし、T［q］は前記キー信号の集合のq番目の要素）の各大きさに基づいて設定するステップと、

前記z信号の大きさを、前記第2の中間信号の集合の第i要素および前記信号zの各大きさに基づいて更新するステップと、

前記出力信号の集合のｉ番目の要素を、前記第２の中間信号の集合の前記第ｉ要素および前記信号ｋの各大きさに基づいて生成するステップとからなることを特徴とする、請求項７に記載の暗号化方法。

【請求項１３】　前記第２の中間信号の集合を解読する前記ステップが、

ｎビット信号ｚを選択された大きさに設定するステップと、

０≦ｉ＜Ｄの範囲の連続する整数値をとるインデックスｉに対し、

ｎビット信号ｑをｚ＃ｍに（ただし、＃はビットごとのブール排他的ＯＲ演算子であり、ｍはｉ　ｍｏｄ　2^n）設定するステップと、

ｎビット信号ｋをＴ［ｑ］に（ただし、Ｔ［ｑ］は前記キー信号の集合の前記ｑ番目のｎビット要素）設定するステップと、

前記第２の中間信号の集合の前記ｉ番目のｎビット要素と前記信号ｚを、2^nを法として加算することによって、前記ｎビット信号ｚの大きさを更新するステップと、

前記第２の中間信号の集合のｉ番目の要素からｎビット信号ｋを、2^nを法として減算することによって、前記出力信号の集合のｉ番目のｎビット要素を生成するステップとからなることを特徴とする、請求項７に記載の暗号化方法。

【請求項１４】　前記各ｎビットが、８ビットで、2^nが２５６に等しいことを特徴とする、請求項１２に記載の暗号化方法。

【請求項１５】　前記メッセージ信号の集合が、セルラ電話システムにおけるメッセージを表すことを特徴とする、請求項１に記載の暗号化方法。

【請求項１６】　前記メッセージ信号の集合が、音声を表すことを特徴とする、請求項１に記載の暗号化方法。

【請求項１７】　前記メッセージ信号の集合が、非音声データを表すことを特徴とする、請求項１に記載の暗号化方法。

【請求項１８】　前記メッセージ信号の集合が、無線通信システムにおけるメッセージを表すことを特徴とする、請求項１に記載の暗号化方法。

【請求項１９】　メッセージを表すメッセージ信号の集合を変換するための暗号化システムにおいて、

第１の中間信号の集合を形成するために、暗号化プロセスおよびキー信号の集合（５０３）によって前記メッセージ信号の集合を暗号化する手段（２１０）と、

第２の中間信号の集合を形成するために、インボリュート変換によって前記第１の中間信号の集合を変更する手段（２１０）と、

出力信号の集合を形成するために、前記暗号化プロセスの逆である解読プロセスによって前記第２の中間信号を解読する手段（２１０）とを有し、

前記変更手段が、前記第１中間信号の集合の第１の部分集合に基づいた非キー変換によって、前記第１の中間信号の集合の第２の部分集合を修正する手段からなることを特徴とする暗号化システム。

【請求項２０】　前記暗号化手段が、第１の自動キープロセスに従って前記第１の中間信号の集合を形成する手段からなり、前記解読手段が、第２の自動キープロセスに従って前記出力信号の集合を形成する手段からなることを特徴とする、請求項１９に記載の暗号化システム。

【請求項２１】　ＮおよびＤを正の整数として、前記キー信号の集合がＮ個の要素を有し、メッセージ信号の集合がＤ個の要素を有することを特徴とする、請求項１９に記載の暗号化システム。

【請求項２２】　前記メッセージ信号の集合を暗号化する前記手段が、

信号ｚを選択された大きさに設定する手段と、

０≦ｉ＜Ｄの範囲の相異なる整数値に信号ｉを設定する手段と、

前記信号ｉおよびｚの各大きさに基づいて信号ｑを設定する手段と、

信号ｋを、前記信号ｑおよびＫ［ｑ］（ただし、Ｋ［ｑ］は前記キー信号の集合のｑ番目の要素）の各大きさに基づいて設定する手段と、

前記第１の中間信号の集合のｉ番目の要素を、前記メッセージ信号の集合の前記第ｉ要素および前記信号ｋの各大きさに基づいて生成する手段と、

前記信号ｚの大きさを、前記第１の中間信号の集合の第ｉ要素および前記信号ｚの各大きさに基づいて更新する手段とからなることを特徴とする、請求項２１に記載の暗号化システム。

【請求項２３】　前記第１の中間信号の集合の前記変更手段が、０≦ｉ＜（Ｄ－１）／２の範囲で、ｂ（ｉ）＃ｑに等しい前記第２の中間信号の集合のｉ番目の要素（ただし、ｂ（ｉ）は前記第１の中間信号の集合のｉ番目の要素であり、ｑはｂ（ｘ）に基づき、ｘはＤおよびｉの値に基づき、ｂ（ｘ）は前記第１の中間信号の集合のｘ番目の要素であり、＃はビットごとのブール排他的ＯＲ演算子）を生成することを特徴とする、請求項２１に記載の暗号化システム。

【請求項２４】　前記第２の中間信号の集合を解読する前記手段が、

信号ｚを選択された大きさに設定する手段と、

０≦ｉ＜Ｄの範囲の相異なる整数に信号ｉを設定する手段と、

前記信号ｉおよびｚの各大きさに基づいて信号ｑを設定する手段と、

信号ｋを、前記信号ｑおよびＫ［ｑ］（ただし、Ｋ［ｑ］は前記キー信号の集合のｑ番目の要素）の各大きさに基づいて設定する手段と、

前記信号ｚの大きさを、前記第２の中間信号の集合の第

ｉ要素および前記信号ｚの各大きさに基づいて更新する手段と、

前記出力信号の集合のｉ番目の要素を、前記第２の中間信号の集合の前記第ｉ要素および前記信号ｋの各大きさに基づいて生成する手段とからなることを特徴とする、請求項２１に記載の暗号化システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、暗号化方法に関し、セルラ電話における通信のプライバシー確保のための暗号システムに関する。

【０００２】

【従来の技術】従来の電話においては、各電話セット（ファックス、モデム等）は、ローカルセントラルオフィスの交換機の１つのポートに、物理的に接続される。接続は、与えられた電話線あるいは電話線の指定のチャネルを介して行われる。電話線の接続はサービス提供者（通常は通信事業者）によって行われ、従ってサービス提供者は、チャネルの通話が加入者によるものであることを確信できる。一方、無線電話での加入者の認証は不確かなものである。

【０００３】米国における現在のセルラ電話構成では、加入者が呼び出しを行うと、課金のためそのセルラ電話がサービス提供者に発信者の身元を通知する。この情報は暗号化されていない。第３者がその時点で盗聴すると、加入者の身元情報が得られてしまう。この情報には、加入者の電話番号、加入者の装置の電気シリアル番号（ＥＳＮ）が含まれている。従って、盗聴者はそのセルラ電話をプログラムして正式な加入者になりすまし、サービスを受けることが可能となる。あるいは、通話中に割り込んで、送信電力を増加させることによって、サービス提供者にある制御コードを送って接続に侵入することもできる。サービス提供者は、接続時および／あるいは通話中の発信者の身元の確認機構を持たないため、このような侵害は基本的に避けられない。

【０００４】盗聴者が身元情報を知ろうとすれば、割当てセル内の全セルラ周波数帯を、自動的に掃引する装置を用いることができる。従って、セルラ電話サービスの侵害を阻止できない。また、音声信号を暗号化していないため、会話の内容を盗聴することができる。つまり、セルラ電話システムにおいて効果的な保護手段が必要とされており、利用者の認証およびプライバシー保護のために、暗号化の利用が必要とされる。

【０００５】

【発明が解決しようとする課題】いくつかの標準的な暗号方法は、セルラ電話等の一般的な認証問題の解決に用いることができるが、実際上の問題もある。まず、プライベートキー暗号アルゴリズムに基づいた、従来の要求／応答プロトコルを用いることができる。この方法では、加入者の移動ステーションに秘密キーが割り当てられ、このキーはホームシステムにも登録されている。提供システムが加入者を認証する場合には、ホームシステムに対して、その加入者の利用に関して照会を行う。ホームシステムは不定期に要求を行い、加入者からのキーを伴う要求に対して、対応する応答を行う機能を果たす。要求および応答は提供システムによって行われ、移動ステーションへの要求も行う。移動ステーションは、要求とその記憶された秘密キーとを処理した結果を応答する。提供システムは、ホームステーションおよび移動ステーションからの応答を比較し、一致した場合に認証されたと見なす。

【０００６】この方法の問題点は、提供システムが発信時の認証の際に、十分早くホームシステムに接続することができず、ホームシステムのデータベースソフトウェアが加入者の秘密キーを調べ、要求／応答ペアを構成することを短期間に行うことができない点である。ネットワークあるいはソフトウェアの数秒の遅延は、加入者が発信する際に、受話器を持ち上げてからダイヤルトーンが聞こえるまでのデッドタイムを増し、さらに（セルラ提供者の現在用いている制御ネットワークおよび交換装置によって）遅延時間が増す。現状では、そのような遅延は許容されない。

【０００７】パブリックキー暗号システムは、認証問題を解決するもう一つの標準的な方法である。一般的に、各移動ステーションはサービス提供者のパブリックキーによって、“パブリックキー証書”が与えられ、その移動ステーションがサービス提供者の合法的な利用者であることを示す。さらに、各移動局に秘密データ（プライベートキー）が与えられ、証書と同時に第３者に合法的な利用者であることを示すのに用いられる。

【０００８】例として、サービス提供者はＲＳＡキーペア（Ｆ，Ｇ）を、Ｆをプライベート、Ｇをパブリックとして有する。サービス提供者は各移動局に、そのＲＳＡキーの独自のペア（Ｄ，Ｅ）を、Ｆ（Ｅ）（提供者のプライベートキーＦを用いて移動局のパブリックキーＥを暗号化したもの）と共に与える。移動局は、提供システムに、（Ｅ，Ｆ（Ｅ））を送ることによってその身元を提示する。提供システムでは、Ｆ（Ｅ）にＧを用いてＥを得る。提供システムは要求Ｘを生成し、移動局のパブリックキーＥを用いて暗号化してＥ（Ｘ）を得て、それを移動局へ送る。移動局は、Ｅ（Ｘ）にプライベートキーＤを用いてＸを得て、解読した状態でそれを応答として提供システムへ返送する。

【０００９】この問題について、処理あるいはデータ伝送量を減少させる改良例もあるが、セルラ電話で現在用いられているハードウェアにおいて、数秒以下で効率的に実行できる、パブリックキー認証方法は存在しない。認証時には、提供システムとホームシステム間でのネットワークの接続性は必要とされないが、従来方法での時間的な制限が問題となるように、パブリックキー方法で

も同様の制約が生じる。

【００１０】

【課題を解決するための手段】本発明では、可変長の元メッセージを、８ビットマイクロコンピュータによって簡単に暗号化および解読を行うことが可能である。本発明は、比較的安全な、自己転換、対称キー暗号システムで、３段階から構成される。第１段階は、元テキストの自動キー暗号化である。第２段階は、自己転換暗号化で、暗号キーは第１段階で暗号化されたメッセージの一部から導出される。第３段階は、第２の自動キー解読で、第１段階の自動キー暗号化に対応する。

【００１１】

【実施例】移動セルラ電話システムでは、多数の移動電話、少数のセルラ無線提供者（各提供者が複数の基地局を有する）、複数の交換ネットワーク提供者（通信事業者）から構成される。セルラ無線提供者と通信事業者は、セルラ電話加入者によって、セルラおよび非セルラ両者の電話加入者との通話を可能にするように組合せられる。図１に概略の構成を示すように、通信事業者ＩおよびＩＩは、交換機１０－１４を有する交換ネットワークを形成して結合される。固定局ユニット２０および２１は交換機１０に接続され、移動局ユニット２２および２３は不特定位置で、基地局３０－４０は交換機１０－１４に接続される。基地局３０－３４は提供者１、基地局３５および３６は提供者２、基地局３７は提供者４、基地局３８－４０は提供者３にそれぞれ属する。本発明の目的では、基地局は複数の送信器を有するセルと同じ意味である。セルの集合体は、図１の基地局３０、３１および３２のように、地理上のセルラサービスエリア（ＣＧＳＡ）を形成する。

【００１２】各移動局ユニットは、そのユニット固有の電気シリアル番号（ＥＳＮ）を有する。ＥＳＮ番号はユニットの製造時に、製造者によって割り当てられ（例えば、ＲＯＭ内に）、アクセスはできるが変更はできない。

【００１３】利用者がその移動電話ユニットのサービスアカウントを申請すると、サービス提供者は利用者に、電話番号（ＭＩＮ１呼称）、エリアコード（ＭＩＮ２呼称）、“秘密キー”（Ａキー）を割り当てる。ＭＩＮ１およびＭＩＮ２呼称は提供者のＣＧＳＡに関連し、図１の構成の全基地局は、特定のＭＩＮ２およびＭＩＮ１ペアの属するＣＧＳＡを識別することができる。Ａキーは、利用者装置および提供者のＣＧＳＡプロセッサ（図１には示さず）だけが知っている。ＣＧＳＡプロセッサは、ユニットのＥＳＮ、Ａキー、ＭＩＮ１およびＭＩＮ２呼称の他、サービス提供者の必要な情報を保持している。

【００１４】ＭＩＮ１呼称およびＡキーがインストールされ、ＣＧＳＡプロセッサが、移動局ユニットに特定のランダムシーケンス（ＲＡＮＤＳＳＤ）を送信し、“共有秘密データ”（ＳＳＤ）の作成を指示することによって、利用者のユニットが初期化される。（ＣＧＳＡは、ＲＡＮＤＳＳＤおよびＳＳＤフィールドの生成を、移動局ユニットの存在するセルの基地局を通して送信する。）ＳＳＤフィールドの作成は図２に示されるプロトコルに従う。

【００１５】図１の構成では、各基地局は、あらかじめ割り当てられたチャネルのいくつかを用いて、そのセル内の全てのユニットに情報を送信する（送信バンド）。さらに、各移動局ユニットに対して、相互に確認した、（一時的に）割り当てられたチャネルによって、双方向通信を確保する。基地局と移動局ユニットで、通信チャネルの確認を行う方法は、本発明には重要でないため、ここでは詳しく述べない。例としては、移動局ユニットが全チャネルをスキャンし開きチャネルを選択する方法が考えられる。その後基地局へ、そのＭＩＮ２およびＭＩＮ１呼称を送信し（元テキストあるいはパブリックキーによって暗号化されたもののいづれか）、基地局に認証プロセスの開始を許可する。認証通信が確立されると、基地局は移動局を他のチャネルへスイッチしても良い。

【００１６】本発明による移動電話システムでの呼び出しの確立と保持方法では、認証プロセスは会話中に多数回行われる。従って、認証プロセスは比較的安全で簡単に行うことができる。設計を簡単にし導入費用を抑えるために、移動局ユニットおよび基地局の両方で同じプロセスを用いるべきである。

【００１７】多くの認証プロセスは、プロセスを行うために、ハッシング機能あるいは一方向機能を用いる。ハッシング機能は、“秘密キー”をサインに変換する、多対一のマッピングを実行する。以下に、簡単で、速く、効果的で、柔軟性のあるハッシング機能の一例を示す。これは、本発明の認証プロセスに好都合であるが、他のハッシング機能を用いることもできる。

【００１８】ジャンブルプロセス

ジャンブルプロセスでは、ｄの“秘密”データワードｂ（ｉ）の“サイン”を、ｋワードのキーｘ（ｊ）によって生成する。ここで、ｄ，ｉ，ｊ，およびｋは整数である。“サイン”の生成プロセスは、１回に一つのデータワードを実行する。この説明のために、ジャンブルプロセスで操作するワードが８ビット長（０から２５６の範囲）であるとするが、他のワードサイズでも実行できる。“秘密”データブロック長を、鋸歯状波関数に用いて、

$s_d(t) = t$　　$0 \leqq t \leqq d-1$

$s_d(t) = 2d-2-t$　　$d \leqq t \leqq 2d-3$

$s_d(t) = s_d(t+2d-2)$　　（全ｔに対して）

とする。この関数は、ｚ＝０およびｉ＝０から始め、０≦６ｄ－５の範囲で連続的に増加する整数ｉに対する以下のプロセスで用いられ、ａ）ｂ（$s_d(i)$）を、ｂ

$(s_d(i))$ b $(s_d(i))$ $+x(i_k)$ $+$SBOX (z) mod256によって更新し、ここで、i_kはi mod k、SBOX $(z)=y+[y/2048]$ mod256、$y=(z\#16)(z+111)(z)$とし、$[y/2048]$はyを2048で割った整数部を示し、#はビット排他OR関数である；b）zを、$z=z+b(s_d(i))$ mod256によって更新する。

【0019】上記のプロセスでは、データとキーの間に明確な区別は無いことが分かる。従って、認証に用いられるどの符号列も、上記のプロセスでキーとして用いられる部分を有することができる。逆に、キーと結合されたデータワードは、“認証”符号列と考えられる。各ワードb（i）は、$0 \leqq i < d-1$で1回に一つそれぞれ分割され、ハッシングを“適切”に行うことができる。ハッシングプロセス自体には、余分のバッファは必要とされない。

【0020】上述のプロセスで必要とされる操作は、シフト（2048による割り算）、切捨て（ ⌊ ⌋ 関数およびmod256関数）、加算、乗算、およびビット排他OR関数であるため、基本的な従来のプロセッサで簡単に実行できる。

【0021】図2のSSDフィールドの初期プロセスに戻って、RANDSSDシーケンスおよび新規のSSDフィールド（図2の矢印）の作成指示が移動ステーションで受信されると、図3に従って新規のSSDフィールドが生成される。移動局ユニットは、ESN呼称、Aキー、RANDSSDシーケンスを結合して認証符号列を形成する。認証符号列はジャンブルブロック101（前述）へ導かれ、SSDフィールドを出力する。SSDフィールドは2つのサブフィールドから構成される：認証手順の補助に用いられるSSD－Aサブフィールド、および音声プライバシー手順およびある信号メッセージ（後述）の暗号化を補助に用いられるSSD－Bサブフィールドである。多数のSSDサブフィールドが生成される。全ビット数を多くする必要がある場合には、データビット数の多いものから始めればよい。以下に述べるように、これは通常必要とされることはない。

【0022】ホームCGSAプロセッサは、受信されたMIN2およびMIN1呼称の割り当てられた移動局ユニットのESNおよびAキーを知っている。また、送信したRANDSSDシーケンスも知っている。従って、ホームCGSAプロセッサでは、移動局ユニットのSSDフィールド生成プロセスを複製する。RANDSSD信号を、ESN呼称およびAキー、前述のジャンブルプロセスと結合することによって、CGSAプロセッサは新規のSSDフィールドを生成し、それをSSD－AおよびSSD－Bのサブフィールドに分割する。しかし、ホームプロセッサで生成されたSSDフィールドは検証されねばならない。

【0023】図2のように、SSDフィールドの検証は移動局ユニットによって行われる。移動局ユニットはブロック102においてランダム要求シーケンス（RANDBSシーケンス）を生成し、サーバ基地局を通じてホームCGSAプロセッサへそれを送信する。図4のように、ホームCGSAプロセッサは、要求RANDBSシーケンス、移動局ユニットのESN、MIN1呼称、新規生成されたSSD－Aを結合し、ジャンブルプロセスで用いられる認証符号列を形成する。この例では、ジャンブルプロセスは、移動局へ送られる分割された認証信号AUTHBSを生成する。移動局はまた、RANDBSシーケンス、ESN呼称、MIN1呼称、新規生成されたSSD－Aを結合し、ジャンブルプロセスで用いられる認証符号列を形成する。移動局は、そのジャンブルプロセスの結果と、ホームCGSAプロセッサからの分割された認証信号（AUTHBS）とを比較する。比較ステップ（ブロック104）で一致すると、移動局は、SSDフィールドの更新に成功したことを示す確認メッセージを、ホームCGSAプロセッサへ送る。一致しない場合には、その比較結果を移動局が送信する。

【0024】移動局が初期化されても、SSDフィールドは、ホームCGSAプロセッサが新規のSSDフィールドを生成することを指示するまで、そのまま保持される。これは例えば、SSDフィールドが処理されたことが認められる場合に生じる。そのような場合、ホームCGSAプロセッサは移動局にもう一つのRANDSSDシーケンスを送り、新規のSSDフィールドを生成するように指示する。

【0025】前述のように、セルラ電話では各基地局から、そのセル内の全ての移動局ユニットのために、種々の情報信号が送信される。図1の構成では、基地局から送信される信号の一つは、ランダムあるいは疑似ランダムシーケンス（RANDシーケンス）である。RANDシーケンスは、移動局ユニットで生成および送信された信号をランダム化して、種々の認証プロセスに用いられる。RANDシーケンスは、録音／再生による妨害を防ぐために定期的に変更されねばならない。RAND信号の待ち時間の設定方法として、予想される平均呼び出し時間より短く設定する方法がある。従って、通常移動局では、連続する呼び出しに対して異なったRAND信号を用いることになる。

【0026】本発明では、移動局ユニットがセルに入るとすぐに、認証されるように基地局ユニットに登録し、移動局からの呼び出しと、基地局からの移動局への呼び出しが行えるようにする。移動局がサーバ基地局に登録されると、サーバ基地局へ、MIN1およびMIN2呼称およびESNシーケンスを送信する。認証プロセスは登録の際に行われ、そのプロセスを図5に示す。図5のように、移動局はRANDシーケンスを受信し；ESNシーケンス、MIN1呼称、SSD－Aサブフィールド

を結合し、ジャンブルプロセスで用いられる認証符号列を形成する。ジャンブルプロセスの出力の、分割された認証符号列は、ＥＳＮシーケンスと共にサーバ基地局へ送られる。

【００２７】ある実施例では、分割された認証符号列が基地局へ届くまでにＲＡＮＤシーケンスが変化する可能性があるため、移動局ユニットで用いられるＲＡＮＤシーケンスの全部あるいは一部もまたサーバ基地局へ送られる。

【００２８】サーバ基地局は、ＲＡＮＤシーケンスを生成したためそれを知っている。基地局はまた、移動局ユニットを識別するための、ＥＳＮ、ＭＩＮ２およびＭＩＮ１呼称をも知っている。しかし、最初の登録時には、サーバ基地局は移動局ユニットのＳＳＤフィールドを知らない。しかし、移動局ユニットのホームＣＧＳＡプロセッサを知っている（ＭＩＮ１およびＭＩＮ２呼称から）ため、認証プロセスは以下のようになる。サーバ基地局は、ホームＣＧＳＡプロセッサに、ＭＩＮ１呼称、ＥＳＮシーケンス、移動局ユニットが送信した分割された認証符号列、分割された認証符号列を生成するために移動局ユニットが用いたＲＡＮＤシーケンスを送信する。移動局ユニットのＭＩＮ１呼称およびＥＳＮシーケンスから、ホームＣＧＳＡプロセッサは、移動局ユニットのＳＳＤ－Ａサブフィールドを知り、前述のように認証符号列を生成し、ジャンブルプロセスへ導く。ホームＣＧＳＡプロセッサによって生成された分割された認証符号列が、移動局ユニットによって生成され、サーバ基地局から送られた分割された認証符号列と一致する場合には、検証は成功したと見なされる。この場合、ホームＣＧＳＡプロセッサは、サーバ基地局にユニットのＳＳＤフィールドを与える。ＥＳＮ呼称およびＳＳＤフィールドの安全を確保するために、基地局とＣＧＳＡプロセッサ間の通信は暗号形式で行われる。

【００２９】移動局ユニットが（前述のプロセスによって）サーバ基地局で認証されると、サーバ基地局は移動局ユニットのＥＳＮおよびＳＳＤフィールドを所有し、そのセル内のその後の認証プロセスはサーバ基地局内で、ホームＣＧＳＡプロセッサを参照することなく進めることができる。ＳＳＤフィールドを更新する際には、ホームＣＧＳＡプロセッサおよび移動局ユニット間で通信し、基地局はそれらの間を取り持つだけとなる。つまり、ホームＣＧＳＡプロセッサは、ＲＡＮＤＳＳＤシーケンスを生成し、ＲＡＮＤＳＳＤシーケンスに基づいてＳＳＤフィールドを更新し、サーバ基地局にＲＡＮＤＳＳＤシーケンスおよび新規に生成されたＳＳＤフィールドを与え、サーバ基地局は、移動局ユニットに、そのＳＳＤフィールドを更新しサーバ基地局に要求を送るように指示し、ＡＵＴＨＢＳ符号列（前述）を生成し、それを移動局ユニットへ送り、移動局ユニットはＡＵＴＨＢＳ符号列を検証し、サーバ基地局へ、移動局ユニットおよびサーバ基地局が同じＳＳＤフィールドを有することを通知する。

【００３０】図６に示すように、サーバ基地局によって登録されると、移動局ユニットは発信することができる。発信シーケンスでは、ＲＡＮＤ、ＥＳＮ、ＳＳＤ－Ａ信号、受信者を識別する（電話）番号を結合する。結合された信号は、サーバ基地局で検証できる、分割された認証シーケンスのために、ジャンブルプロセスへ送られる。基地局で検証できるように、受信者の識別番号（および前述のＲＡＮＤ信号の一部）は基地局で受信できるような状態、つまり元テキストでも送信されねばならない。認証シーケンスが検証されると、基地局は発信を処理し、受信者との接続を行う。

【００３１】移動局ユニットが“受信者”である場合の接続プロトコルは、図５の登録プロトコルに従う。つまり、サーバ基地局が呼び出された移動局に、ＲＡＮＤシーケンス、ＥＳＮ呼称、ＭＩＮ１呼称およびＳＳＤ－Ａサブフィールドから生成された認証シーケンスを送信するように要求する。認証されると、基地局と受信者の移動局ユニット間に経路が設定され、発信した移動局（あるいは固定局）とのデータのやり取りを行えるようにする。

【００３２】上記の認証は（検証されることを考慮して）、認証されたパケットあるいは符号列それ自身に関してのみ有効である。それ以外に安全性を高めるには、３つの異なった追加保護手段が用いられる。これらは、音声暗号化、不定期の再認証、制御メッセージの暗号化である。

【００３３】音声暗号化

音声信号は第１に、デジタル形式にすることで暗号化される。これは、圧縮の有無、誤り訂正コードの有無を問わず種々の従来方法で行うことができる。デジタル信号のビットはＫビット毎のグループに分割され、各グループが暗号化される。移動局ユニットおよび基地局において、ＲＡＮＤシーケンス、ＥＳＮおよびＭＩＮ１呼称、ＳＳＤ－Ｂサブフィールドが結合され、ジャンブルプロセスへ導かれる。ジャンブルプロセスでは２Ｋビットが作られ、Ｋビット毎のグループＡおよびＢに分けられる。移動局ユニットのグループＡは出力音声の暗号化に用いられ、グループＢは入力音声の解読に用いられる。一方、基地局ではグループＡは入力音声の解読に用いられ、グループＢは出力音声の暗号化に用いられる。図７に音声の暗号化および解読プロセスを示す。

【００３４】再認証

基地局では、再認証プロセスによって、基地局が動作を検知した移動局ユニットが、本当に動作を認可された移動局ユニットであるかを確認する。これは、図８に示されるように、基地局が移動局ユニットに、分割された認証シーケンスを送信するように要求すれば良い。そのような各要求に対して、基地局は特別（ＲＡＮＤＵ）シー

ケンスを送信する。移動局ユニットは、ＲＡＮＤＵシーケンス、移動局ユニットのエリアコードＭＩＮ２呼称、ＥＳＮ呼称、ＭＩＮ１呼称、ＳＳＤ－Ａ呼称を結合して、分割された認証シーケンスを生成する。結合された符号列は、ジャンブルプロセスへ導かれ、その結果得られた、分割された認証符号列が基地局へ送信される。この地点で基地局は、分割された認証符号列が有効であるかどうかを検証する。

【００３５】制御メッセージ暗号システム

第３の安全方法では、制御メッセージを保護する。通話中には、種々の状況において、制御メッセージを伝える必要がある。ある場合には、制御メッセージは、発信した移動局あるいは基地局のどちらかに重大な悪影響を及ぼす可能性がある。そのため、通話中に送られるある種の制御メッセージは（十分に）暗号化されていることが望ましい。あるいは、ある種のメッセージ形式のあるフィールドを暗号化しても良い。これには、クレジットカード番号のような“データ”制御メッセージおよび発信再定義制御メッセージが含まれる。これは、制御メッセージ暗号システムによって行われる。

【００３６】制御メッセージ暗号システム（ＣＭＣ）は対称キー暗号システムで、以下の特徴を有する：１）比較的安全、２）８ビットコンピュータで効率良く動作する、３）自己転換である（すなわちインボリュート）。

【００３７】ＣＭＣの暗号キーは、２５６バイトの配列ＴＢＯＸ［ｚ］で、“秘密キー”（例ＳＳＤ－Ｂサブフィールド）から以下のように導かれる：０≦ｚ＜２５６の範囲の各ｚに対して、ＴＢＯＸ［ｚ］＝ｚと設定し、配列ＴＢＯＸ［ｚ］および秘密キー（ＳＳＤ－Ｂ）をジャンブルプロセスへ導く。これは本質的に、図７の要素３０１、３０２および３０３に示されるものである（ただし、図７のバイト数は２５６ではなく２Ｋである）。

【００３８】キーが導かれると、ＣＭＣは制御メッセージの暗号化および解読に用いることができる。あるいは、キーの用いられる各時間に、“素早く”キーを導くことも可能である。ＣＭＣは複数バイトの可変長メッセージの暗号化を行うことができる。ＣＭＣの動作は、自己転換で、相互的あるいはインボリュートである。つまり、元テキストを暗号化されたテキストから得るための操作と、元テキストを暗号化したテキストを得るための操作とは完全に同じである。インボリュート関数は、それ自身の逆関数である（例、ｘ＝１／ｘ’，ｘ＝Ｔ（Ｔ（ｘ’））。従って、ＣＭＣ操作を２回行っても、バッファの内容は変化しない。

【００３９】以下の説明では、暗号化プロセス（解読プロセス）では、元のテキスト（暗号化されたテキスト）がデータバッファ内に保持され、ＣＭＣはデータバッファ内の内容を操作して、データバッファの内容が最終的に暗号化されたテキスト（あるいは解読されたテキスト）を構成することを仮定する。これは、図９の要素５０２および５０４が一つの同じレジスタで良いことを示す。

【００４０】ＣＭＣは連続する３つの段階から構成され、それぞれデータバッファ内の各バイト符号列を更新する。全体としてのＣＭＣおよびＣＭＣの第２段階はインボリュートである。データバッファがｄバイトで、ｉを０≦ｉ＜ｄの範囲として、各バイトをｂ（ｉ）で表す：ＣＭＣの第１段階は以下のようになる：ｚの初期値を０とし、ｉを０≦ｉ＜ｄの範囲の整数として、変数ｑを：ｑ＝ｚ＃ｉの低位バイトとし、ここで、＃はビットブール排他ＯＲ演算子とし、変数ｋを：ｋ＝ＴＢＯＸ［ｑ］とし、ｂ（ｉ）を：ｂ（ｉ）＝ｂ（ｉ）＋ｋ　ｍｏｄ　２５６によってアップデートし、ｚを：ｚ＝ｂ（ｉ）＋ｚ　ｍｏｄ　２５６によって更新する。ＣＭＣの第２段階はインボリュートで、０≦ｉ＜（ｄ－１）／２の範囲の全てのｉに対して、ｂ（ｉ）＝ｂ（ｉ）＃（ｂ（ｄ－１－ｉ）　ＯＲ　１）によって処理し、ここでＯＲはビットブール排他ＯＲ演算子である。ＣＭＣの最終段階は、第１段階に対して逆となる解読プロセスで：ｚの初期値を０とし、ｉを０≦ｉ＜ｄの範囲の整数として、変数ｑを：ｑ＝ｚ＃ｉの低位バイトとし、変数ｋを：ｋ＝ＴＢＯＸ［ｑ］とし、ｚを：ｚ＝ｂ（ｉ）＋ｚ　ｍｏｄ　２５６によって更新し、ｂ（ｉ）を：ｂ（ｉ）＝ｂ（ｉ）－ｋ　ｍｏｄ　２５６によって更新する。図９に、選択された制御およびデータメッセージの暗号化および解読の、３段階のプロセスを示す。実施例では、第１段階および第３段階はそれぞれ、自動キー暗号化、解読プロセスである。自動キーシステムは、システムの出力がその後のシステム出力に影響するような、時間変化するシステムである。暗号化および自動キーシステムの詳細については、W.Diffie and M.E.Hellman, Privacy and Authentication: An Introduction to Cryptography, Proc. of the I.E.E.E.,Vol.67,No.3, March 1979を参照のこと。

【００４１】移動局ユニット装置

図１０に移動局ユニットのハードウェアのブロック図を示す。制御ブロック２００は、セルラ電話キーパッド、ハンドセット、ユニット電源制御スイッチ化ら構成される。制御ブロック２００は、プロセッサ２１０へ接続され、音声信号のデジタル化、誤り訂正コードの組み入れ、デジタル音声信号の暗号化、入力音声信号の解読、種々の制御メッセージの形成および暗号化（解読）等を行うために、移動局ユニットの動作を制御する。ブロック２１０は、信号の送受信回路からなるブロック２２０へ結合される。ブロック２００－２２０は基本的に従来方法のブロックで、現在市販の移動電話ユニット（市販のユニットでは暗号化および解読は行われない）の機能を達成するものである。本発明の認証および暗号化プロセスのために、図８の装置にはさらに、多数のレジスタ

をプロセッサ２１０へ結合したブロック２４０が含まれ、“個別”モジュール２３０もプロセッサ２１０へ結合される。モジュール２３０は、移動電話ユニットの一部であるか、ソケットによって移動電話ユニットに着脱可能なモジュールであっても良い。モジュールは、電磁的にあるいは接続によってプロセッサ２１０へ接続される。モジュール２３０は例えば、“スマートカード”でも良い。

【００４２】モジュール２３０は、ジャンブルプロセッサ２３１およびプロセッサ２３１の多数のレジスタから構成される。あるいは、他の実施例では、Ａキーのみをモジュール２３０に配置しても良い。Ａキー、ＭＩＮ１およびＭＩＮ２呼称をブロック２４０のレジスタよりは、モジュール２３０のレジスタにインストール（および保持）する方が都合が良い。また、得られたＳＳＤフィールドをモジュール２３０のレジスタに記憶させるのも好都合である。プロセッサ２３１の処理を実行するのに必要なレジスタを、モジュール２３０内に配置することが好ましい。モジュール２３０にこれらの要素を配置することによって、利用者はモジュールを持ち運んで異なった移動ユニットに用いることができ（例として、“拡張”移動ユニット）、より重要な情報の多くをモジュール以外に記憶させることができる。移動ユニットは、ユニットと一体化したモジュール２３０としても良い。そのような実施例では、ジャンブルプロセッサ２３１はプロセッサ２１０内に組み込まれる。ブロック２４０では、受信されるユニットのＥＳＮ呼称および種々のＲＡＮＤシーケンスを保持する。

【００４３】本発明は、セルラ電話における加入者の認証に関するものであるが、ポータブルハンドセットを用いるパーソナル通信ネットワークも包含し、本発明の原理は、通信の安全性が十分に確保されない場合や、偽装者が問題となる場合にも有効である。例えば、コンピュータネットワークも含まれる。

【００４３】

【発明の効果】以上に述べたように、本発明では、セルラ電話システムにおける暗号システムにおいて、可変長の元メッセージを、８ビットマイクロコンピュータによって簡単に暗号化および解読を行うことが可能な、比較的安全な、自己転換、対称キー暗号システムを提供することができる。

【図面の簡単な説明】

【図１】固定および移動電話の両方のサービスのために相互接続された、ネットワーク提供者およびセルラ無線提供者の構成を示す図である。

【図２】共有秘密データフィールドの作成と同一性の検証を行うプロセスを示す図である。

【図３】共有秘密データ作成のための各要素の接続および分割を示す図である。

【図４】検証シーケンス作成のための各要素の接続および分割を示す図である。

【図５】移動局ユニットの送信中の登録シーケンス作成のための各要素の接続および分割を示す図である。

【図６】呼び出しシーケンス作成のための各要素の接続および分割を示す図である。

【図７】移動局ユニットでの音声の暗号化および解読プロセスを示す図である。

【図８】再認証シーケンス作成のための各要素の接続および分割を示す図である。

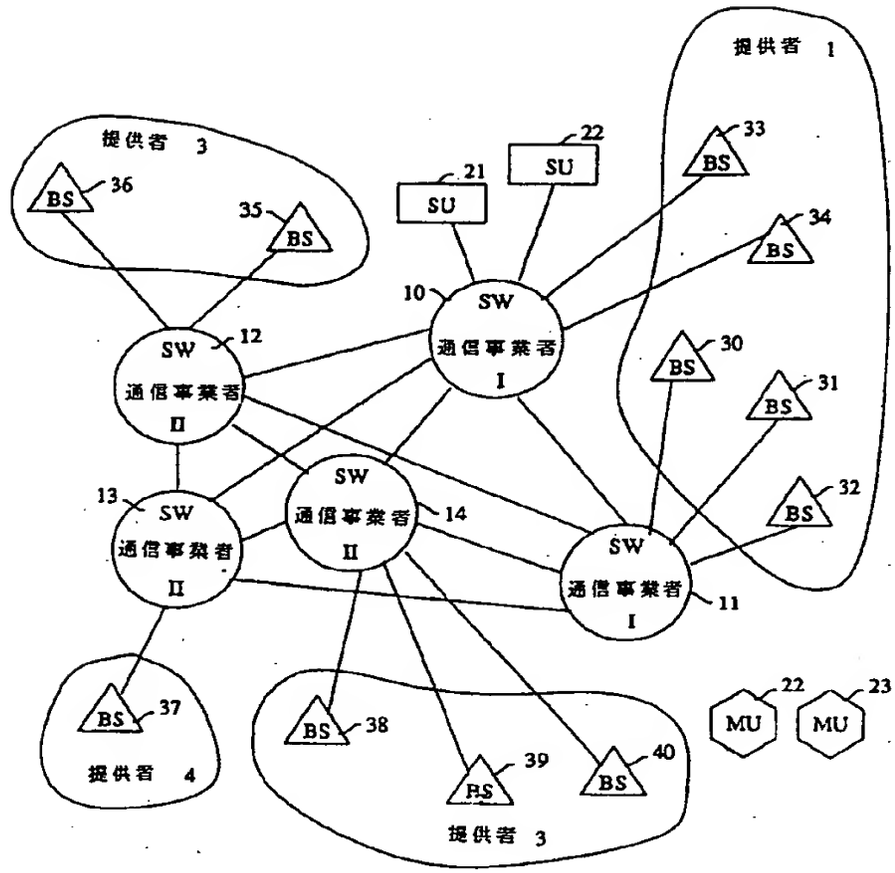
【図９】選択された制御およびデータメッセージの暗号化および解読のための３段階のプロセスを示す図である。

【図１０】移動局ユニットのハードウェアのブロック図である。

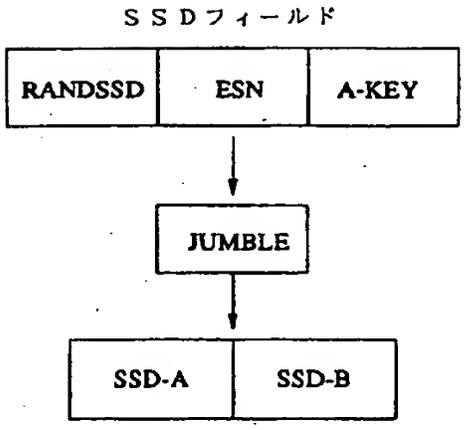
【符号の説明】

１０－１４　交換機
２０－２１　固定局
２２－２３　移動局
３０－４０　基地局
１０１　ジャンブルブロック
１０２　ブロック
１０４　ブロック
２００　制御ブロック
２１０　プロセッサ
２２０　ブロック
２３０　モジュール
２３１　プロセッサ
２４０　ブロック
３０１－３０３　要素
５０２　要素
５０４　要素

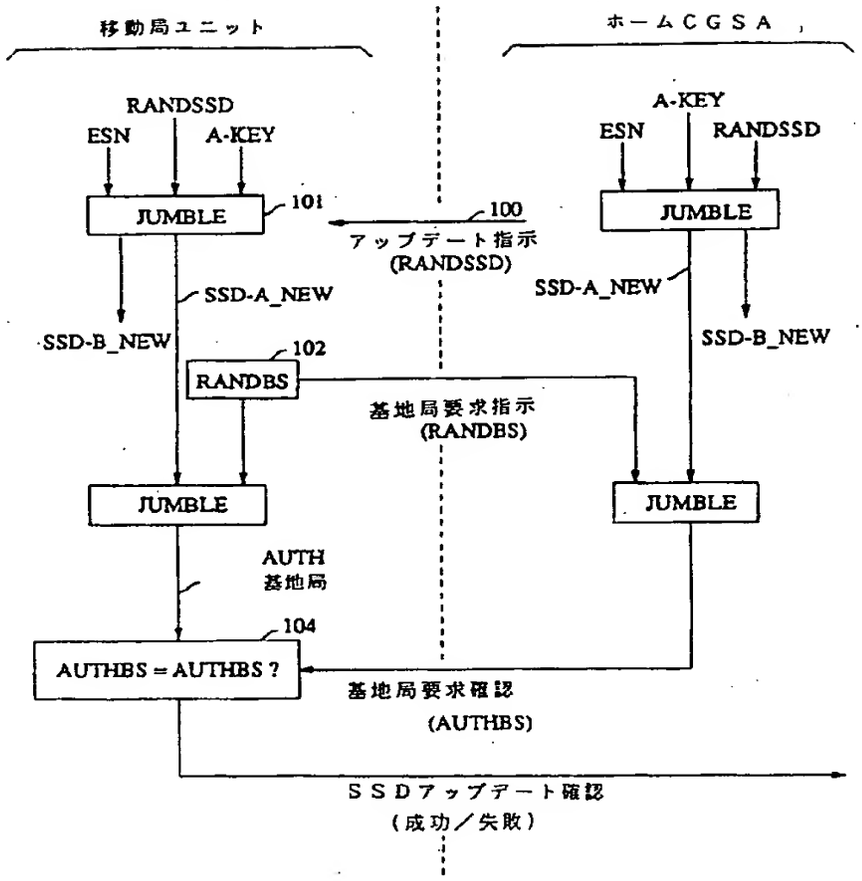
【図1】


提供者 1
提供者 3
提供者 4
提供者 3
SU
SU
BS
SW
通信事業者
I
SW
通信事業者
II
SW
通信事業者
II
SW
通信事業者
II
SW
通信事業者
I
MU
MU
10
11
12
13
14
21
22
23
30
31
32
33
34
35
36
37
38
39
40

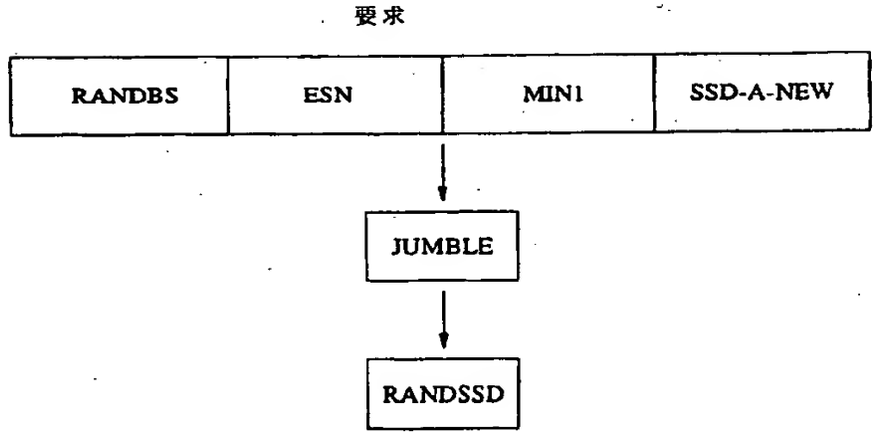
【図3】


ＳＳＤフィールド
RANDSSD
ESN
A-KEY
JUMBLE
SSD-A
SSD-B

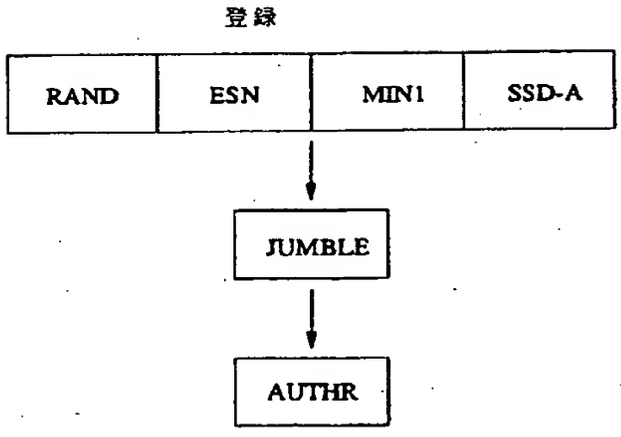
【図2】


移動局ユニット
ホームCGSA
RANDSSD
ESN
A-KEY
A-KEY
ESN
RANDSSD
JUMBLE
101
100
JUMBLE
アップデート指示
(RANDSSD)
SSD-A_NEW
SSD-A_NEW
SSD-B_NEW
SSD-B_NEW
102
RANDBS
基地局要求指示
(RANDBS)
JUMBLE
JUMBLE
AUTH
基地局
104
AUTHBS = AUTHBS ?
基地局要求確認
(AUTHBS)
SSDアップデート確認
(成功／失敗)

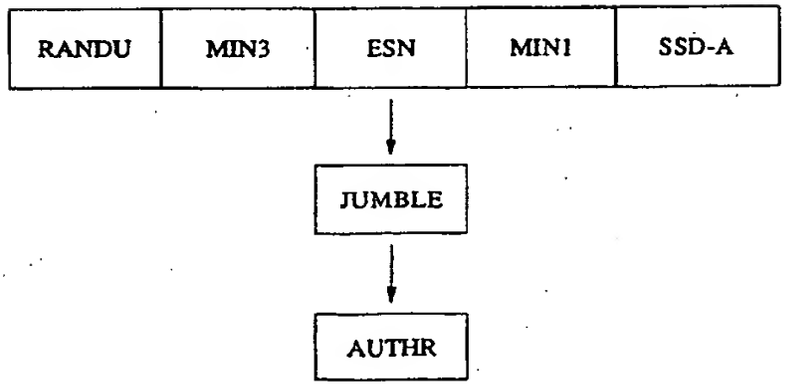
【図4】


要求
RANDBS
ESN
MIN1
SSD-A-NEW
JUMBLE
RANDSSD

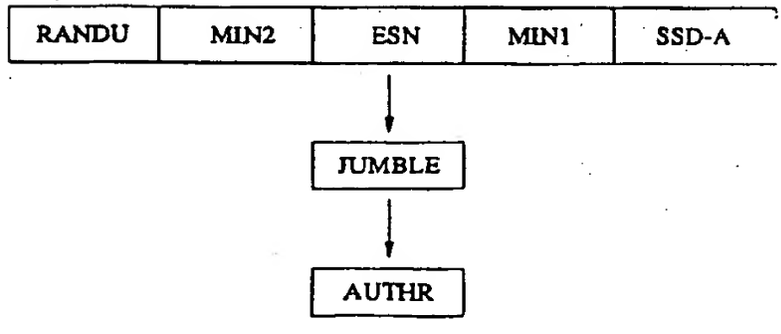
【図5】


登録
RAND
ESN
MIN1
SSD-A
JUMBLE
AUTHR

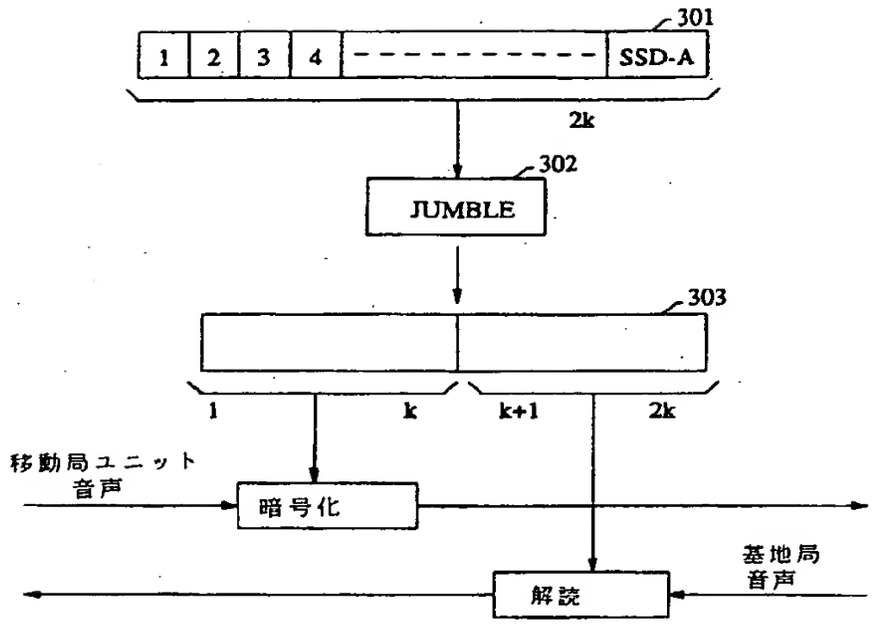
【図6】


RANDU
MIN3
ESN
MIN1
SSD-A
JUMBLE
AUTHR

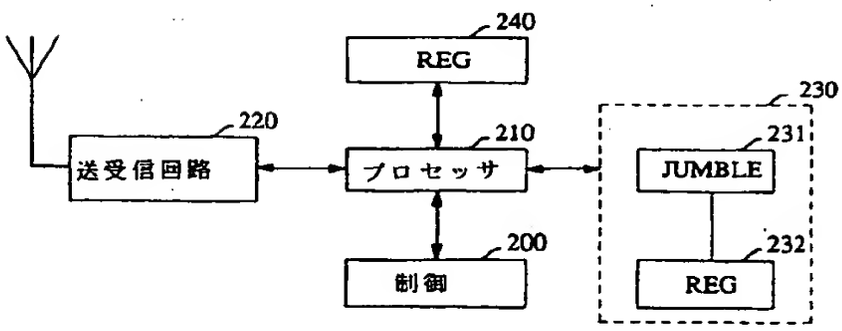
【図8】


RANDU
MIN2
ESN
MIN1
SSD-A
JUMBLE
AUTHR

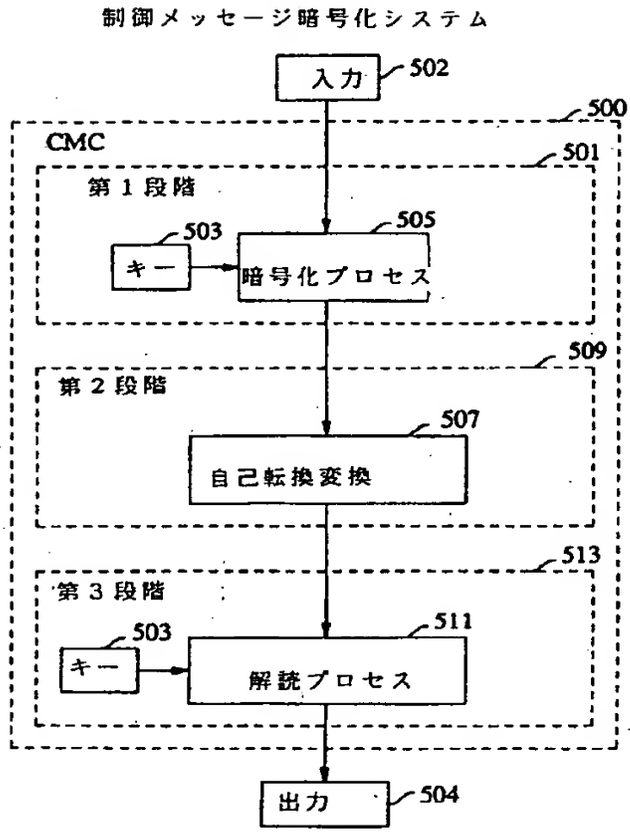
【図7】


301
1
2
3
4
SSD-A
2k
302
JUMBLE
303
1
k
k+1
2k
移動局ユニット
音声
暗号化
基地局
音声
解読

【図10】


240
REG
230
220
210
231
送受信回路
プロセッサ
JUMBLE
200
232
制御
REG

【図9】



フロントページの続き

(72)発明者　ジェームス　アレクサンダー　リーズ　サード
アメリカ合衆国　07974　ニュージャージー　ニュー　プロヴィデンス、サウスゲート　ロード　127